

§1. p 進数の特徴付け

1. \mathbb{Z} の p 進数に付与される
2. \mathbb{Z} の p 進数
3. $\lambda_{m,n} : \mathbb{Z}/p^m\mathbb{Z} \rightarrow \mathbb{Z}/p^n\mathbb{Z} (m \leq n)$ の射影性
4. $\hat{\mathbb{Z}}$ の p 進数

§2. Furstenberg 位相 $\hat{\mathbb{Z}}$

1. Furstenberg 位相
2. $\hat{\mathbb{Z}}$ の位相

§3. p 進数と不定方程式

1. Hensel の補題
2. Hasse - Minkowski の定理

§4. p 進解析の概り

§ 1

1. \mathbb{Z} の p (対 p) による定数化

Def

$\leftarrow p \in \mathbb{Z}$ の
 \leftarrow 互いに素.
 $\bullet \forall a \in \mathbb{Z}^* \text{ には } a = p^{\alpha} \frac{c}{b} (p \nmid b, c) \text{ とかけられる}$

もし、 a の素因数 p に同じものが α 個ある、 $\text{ord}_p a = \alpha$

$\bullet \text{ord}_p 0 = \infty$ とする。更に、 $|a|_p = p^{-\text{ord}_p a}$ 、 $|0|_p = 0$ と
 定める。

Def: $\forall x, y \in \mathbb{Q}, d_p(x, y) = |x - y|_p$

Prop: (\mathbb{Q}, d_p) は、距離空間 になる。

proof

$$(i) d_p(x, y) = p^{-\text{ord}_p(x, y)} \geq 0$$

$$d_p(x, y) = 0 \Rightarrow x = y$$

$$(ii) d_p(x, y) = d_p(y, x)$$

$$(iii) \forall x, y, z \in \mathbb{Q}$$

$$\bullet d_p(x, z) = d_p((x-y) + (y-z))$$

$$\bullet \text{ord}_p \{ (x-y) + (y-z) \}$$

$$\geq \min \{ \text{ord}_p(x-y), \text{ord}_p(y-z) \} \quad \text{ultra metric}$$

$$\bullet d_p(x, z) \leq \max \{ d_p(x-y), d_p(y-z) \}$$

$$\leq d_p(x-y) + d_p(y-z)$$

claim

・ \mathbb{Q} は n , $2-2-\dots$ の \mathbb{Z} である. $\mathbb{Q} \neq (\mathbb{Z} \text{ かつ } \sqrt{5} \notin \mathbb{Z})$

・ $5^m \in \mathbb{Z}^+$.

$$a_n = 2^{5^n} \quad (n=0, 1, 2, \dots) \quad \pm \sqrt{5} \notin \mathbb{Z}$$

$$2^5 \equiv 2 \pmod{5}$$

$$2^{5^2} \equiv 2^5 \pmod{5^2}$$

$$2^{5^R} \equiv 2^{5^{R-1}} \pmod{5^R}$$

$$b = \frac{2^{5^R} - 2^{5^{R-1}}}{5^R} \in \mathbb{Z} \quad \mathbb{Z}^+$$

$$a_n = 2 + \sum_{R=1}^n b \cdot 5^R \quad \text{は、} 2-2-\dots \text{の}$$

(2)

$$\forall m \geq m \quad \text{is } \mathbb{Z}$$

$$\left(\begin{aligned} \text{ord}_p(a_n - a_m) &= \text{ord}_p \left(\sum_{k=m}^n b \cdot 5^k \right) \\ &\geq 5^m \xrightarrow{m \rightarrow \infty} \infty \end{aligned} \right)$$

$\mathbb{Q} \neq \mathbb{Z} \pm \alpha \sqrt{5}$

$$a_{n+1} = a_n^5$$

$$\alpha = 2^5$$

$$\alpha \equiv 2 \pmod{5} \quad \text{or}$$

$$\alpha^4 = 1$$

$$\therefore \alpha = \pm 1 \quad \text{is not}$$

Def 1

- ・ \mathbb{Q} の p 進数体 \mathbb{Q}_p (p 進数体)
- ・ \mathbb{Z} の p 進数体 \mathbb{Z}_p (p 進整数) def

Prop

- ・ \mathbb{Z}_p は \mathbb{Q}_p の p 進数体, \mathbb{Q}_p は \mathbb{Z}_p の p 進数体

proof

- ・ \mathbb{Z}_p (p 進数) の p 進数

$$\begin{aligned} x+y &= \lim_{n \rightarrow \infty} (x_n + y_n) \\ xy &= \lim_{n \rightarrow \infty} x_n \cdot y_n \end{aligned} \quad \left\{ \begin{array}{l} \text{def + dir. ring の収束性から} \end{array} \right.$$

- ・ 収束の連続性により、 $x_n \rightarrow x, y_n \rightarrow y$ のとき

$$x_n + y_n \rightarrow x + y \text{ を示せる。}$$

$$\forall \varepsilon > 0, \exists N, m \geq N, |x_n - x|_p < \varepsilon, |y_n - y|_p < \varepsilon \text{ のとき}$$

$$|(x_n + y_n) - (x + y)|_p = |(x_n - x) + (y_n - y)|_p \leq \max\{|x_n - x|_p, |y_n - y|_p\} < \varepsilon$$

→ 収束性。証明。

Remark, \mathbb{Z}_p の基底は何? ?

$$B_\varepsilon(a) = \{x \in \mathbb{Z}_p \mid |x - a|_p < \varepsilon\}$$

$$|x-a|_p \leq \varepsilon = p^{-e} \ (e \in \mathbb{Z})$$

$$\therefore p^{-\text{ord}_p(x-a)} \leq p^{-e}$$

$$\therefore \text{ord}_p(x-a) \geq e$$

$$x-a \in p^e \mathbb{Z}_p$$

$$\therefore x \in a + p^e \mathbb{Z}_p$$

すなわち $a + p^e \mathbb{Z}_p \ (e \geq 0)$ は \mathbb{Z}_p の基底

2. \mathbb{Z}_p の表現

$$\left\{ \sum_{i=0}^{\infty} a_i p^i \mid 0 \leq a_i \leq p-1 \right\} \subset \mathbb{Z}_p \quad \text{を示す}$$

$$\text{②に、} \forall a \in \mathbb{Z}_p, \exists! a_0, a_1, \dots \in \mathbb{F}_p, a = \sum_{i=0}^{\infty} a_i p^i$$

(\rightarrow 1位元)

Def 2.

$$\mathbb{Z}_p := \left\{ \sum_{i=0}^{\infty} a_i p^i \mid 0 \leq a_i \leq p-1 \right\}$$

$$\mathbb{Q}_p := \left\{ \sum_{i=-m}^{\infty} a_i p^i \mid 0 \leq a_i \leq p-1 \right\}$$

(真)

Th. \mathbb{Z}_p

$$\sum_{n=0}^{\infty} a_n \text{ is convergent } \Leftrightarrow \lim_{n \rightarrow \infty} |a_n|_p = 0$$

$$\left(\lim_{n \rightarrow \infty} \text{ord}_p a_n = \infty \right)$$

proof

$$(\Rightarrow) \quad \checkmark \quad \text{if it is} \quad s_m = \sum_{n=0}^m a_n \quad \text{is convergent}$$

$$|a_n|_p = |s_n - s_{n-1}|_p \xrightarrow{n \rightarrow \infty} 0$$

$$(\Leftarrow) \quad m \geq n \quad \text{ord}_p(s_m - s_n) = \text{ord}_p\left(\sum_{i=n}^m a_i\right)$$

$$\text{ultra} \rightarrow \geq \min \{ \text{ord}_p a_{n_1}, \dots, \text{ord}_p a_{n_k} \}$$

$$n \rightarrow \infty \rightarrow \infty$$

3. 射影极限

$$f = a_0 + a_1 p + a_2 p^2 + \dots \in \mathbb{Z}_p \text{ is } \mathbb{Z}_p$$

$$\bar{s}_1 \equiv a_0 \pmod{p}$$

$$\bar{s}_2 \equiv a_0 + a_1 p \pmod{p^2}$$

射影极限列:

$$\text{is convergent } (\bar{s}_1, \bar{s}_2, \dots) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \dots$$

$$s \geq n, \quad s_{n+1} \equiv s_n \pmod{p^n} \text{ となる}$$

$$\lambda_{m,n} : \mathbb{Z}/p^n\mathbb{Z} \rightarrow \mathbb{Z}/p^m\mathbb{Z} \quad (m \geq n) \text{ となる.}$$

$$\text{例: } \mathbb{Z}/p\mathbb{Z} \leftarrow \mathbb{Z}/p^2\mathbb{Z} \leftarrow \mathbb{Z}/p^3\mathbb{Z} \leftarrow \dots \text{ となる.}$$

この図式は可換に
なる。

$$\begin{array}{ccccccc} \mathbb{Z}/p\mathbb{Z} & \leftarrow & \mathbb{Z}/p^2\mathbb{Z} & \leftarrow & \mathbb{Z}/p^3\mathbb{Z} & \leftarrow & \dots \\ \downarrow & & \downarrow & & \downarrow & & \\ s_1 & & s_2 & & s_3 & & \\ & \nearrow & \nearrow & \nearrow & \nearrow & & \\ & & X & \ni & (\dots, s_1, s_0) & & \\ & & \downarrow & & & & \\ & & \prod_{n \geq 0} \mathbb{Z}/p^n\mathbb{Z} & \ni & (\dots, s_1, s_0) & & \end{array}$$

つまり、

$$X = \left\{ (x_n) \in \prod_{n \geq 0} \mathbb{Z}/p^n\mathbb{Z} \mid \lambda_{m,n}(x_m) = x_n \right\} \text{ となる.}$$

ここで、 \mathbb{Z}_p と同一視する。

Def 3.

図 Top ring における図式 $\mathbb{Z}/p\mathbb{Z} \leftarrow \mathbb{Z}/p^2\mathbb{Z} \leftarrow \mathbb{Z}/p^3\mathbb{Z} \leftarrow \dots$ の

極限を \mathbb{Z}_p と定義する。

1/3. $\mathbb{Z}/p^n\mathbb{Z}$ には、離散位相 を入れたら、

$\mathbb{Z}/p^n\mathbb{Z}$ は、有限集合なので、112117が $\mathbb{Z}/p^n\mathbb{Z}$ 。

2. $\prod_{n \geq 0} \mathbb{Z}/p^n\mathbb{Z}$ は、112117が $\mathbb{Z}/p^n\mathbb{Z}$ 。

$$\text{2.2. } Y = \left\{ (x_n) \in \prod_{n \geq 0} \mathbb{Z}/p^n\mathbb{Z} \mid \lambda_{m,n} \circ p_n(x_n) = p_m(x_m) \right\} \quad (m \geq n)$$

2.2.2.

$$X = \varprojlim \mathbb{Z}/p^n\mathbb{Z} \quad \mathbb{Z}/p^n\mathbb{Z} \leftarrow \mathbb{Z}/p^{n+1}\mathbb{Z}$$

$$X = \bigcap_{n \geq 0} Y$$

lem.

$$X, Y = \text{Top}, \quad Y: 112117$$

$$X \xrightleftharpoons[f]{f} Y: \text{conti}(\mathbb{Z})$$

$$\text{eq}(f, g) = \{x \in X \mid f(x) = g(x)\} \text{ is closed}$$

↑
f, g: $\mathbb{Z} \rightarrow \mathbb{Z}$

lem 2. Y is closed, 2.2. X is closed.

3. $\prod \mathbb{Z}/p^n\mathbb{Z}$ は、112117が $\mathbb{Z}/p^n\mathbb{Z}$ 。

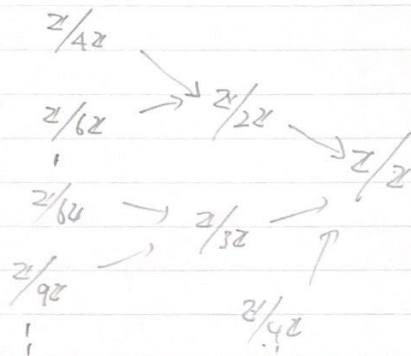
X は、112117が $\mathbb{Z}/p^n\mathbb{Z}$ 。

4. さらに、 \mathbb{Z}_p は、完全不連続 (連続部分 1 と等しい)

- Def: 位相群 G が、任意のコンパクト部分群 H が

完全不連続の時、 G は 副有限群 といい

- Def: Topology により $\lambda_{m,n}: \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ ($m|n$)
から与えられる。



の極限は、 $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/m\mathbb{Z}$ と定義する。

、 $\hat{\mathbb{Z}}$ は、副有限群であり、 $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/m\mathbb{Z}$ は

\mathbb{Z} の 副有限完備化 ($m\mathbb{Z}$ は、 \mathbb{Z} の非ゼロ有限部分群の逆のイデアル) といい。

、 $\forall m \in \mathbb{N}$, $m = p_1^{e_1} p_2^{e_2} \dots$ (素因数分解) とすると

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \mathbb{Z}/p_2^{e_2}\mathbb{Z} \times \dots$$

↑
中国剰余定理

$$\therefore \varprojlim_{\leftarrow} \mathbb{Z}/n\mathbb{Z} \simeq \varprojlim_{\leftarrow} \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \varprojlim_{\leftarrow} \mathbb{Z}/p_2^{e_2}\mathbb{Z} \times \cdots$$

$$\therefore \hat{\mathbb{Z}} \simeq \prod_{p \text{ prime}} \mathbb{Z}_p$$

- Def 4 :

$\hat{\mathbb{Z}}$ の p -adic 成分 \mathbb{Z}_p を def 1

例 2 (Furstenberg 位相) $\hat{\mathbb{Z}}$

- Def

$$a, b \in \mathbb{Z}$$

$$Na, b := \{a + bm \mid m \in \mathbb{Z}\} \text{ は } \hat{\mathbb{Z}} \text{ における Top を作る.}$$

これは (F) 位相である。

- Th. 定理は、位相にある。

proof

$$\{ \pm 1 \} = \mathbb{Z} \setminus \bigcup_p p\mathbb{Z}$$

$\{ \pm 1 \}$ は、有限集合である。open である。

また、 $\bigcup_p p\mathbb{Z}$ は、closed である。

$$\therefore p\mathbb{Z} = \mathbb{Z} \setminus \bigcup_{i=0}^{p-1} Na, i \quad \text{すなわち } p\mathbb{Z} \text{ は closed.}$$

↑
 $p \nmid a, i$ $a \not\equiv i \pmod{p}$ $0 \leq i < p-1$

また、 $\{ \pm 1 \} = \mathbb{Z} \setminus \bigcup_p p\mathbb{Z}$ は closed である。

2. $\hat{\mathbb{Z}}$ の関係

今日の目標は、これを示すこと。

Claim : \mathbb{N} 位相は、 $\hat{\mathbb{Z}}$ の位相と一致する。

$$\hat{\mathbb{Z}} \subseteq \prod_p \mathbb{Z}_p$$

$\prod_p \mathbb{Z}_p$ の基底を知りたい。

\mathbb{Z}_p の基底として、 $a_i + p_i^{e_i} \mathbb{Z}_p$ ($a_i \in \mathbb{Z}_p, e_i \geq 0$) が知られる。

$\prod_p \mathbb{Z}_p$ の基底は、 $(a_1 + p_1^{e_1} \mathbb{Z}_{p_1}) \times (a_2 + p_2^{e_2} \mathbb{Z}_{p_2}) \times \dots$

$$\dots \times (a_n + p_n^{e_n} \mathbb{Z}_{p_n}) \times \prod_{i \neq 1, 2, \dots, n} \mathbb{Z}_{p_i} \quad \text{--- ①}$$

中国剰余定理より、 $\exists a \in \mathbb{Z}, a \equiv a_i \pmod{p_i^{e_i} \mathbb{Z}_{p_i}} \quad (i=1, \dots, n)$

$$\text{① は、 } a + p_1^{e_1} \mathbb{Z}_{p_1} \times p_2^{e_2} \mathbb{Z}_{p_2} \times \dots \times p_n^{e_n} \mathbb{Z}_{p_n} \times \prod_{i \neq 1, \dots, n} \mathbb{Z}_{p_i}$$

よって、 $b = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}$ とおけば、

$\prod_p \mathbb{Z}_p \cap \mathbb{Z}$ の基底は、 $\{a + bn \mid n \in \mathbb{Z}\}$ とおける。

例 3. p 素数 と 不定方程式

・問題

(1) p 奇素数, $\exists x, y \in \mathbb{Q}$, $p = x^2 + y^2$ なる条件は?

(2) $\underbrace{(1, 1, 1, \dots, 1)}_{m \text{ 回}}$ なる 3 重割り切れる問題

$= (m \text{ 回 } 3 \text{ 重割り切れる問題})$

1. Hensel の補題

Th. $f(x) \in \mathbb{Z}_p$ の多項式

$\exists x_0 \in \mathbb{Z}_p$, $\delta_1 := \text{ord}_p(f(x_0))$, $\delta_2 := \text{ord}_p(f'(x_0))$,

$\delta_1 > 2\delta_2 \Rightarrow \exists x \in \mathbb{Z}_p$, $f(x) = 0$, $x \equiv x_0 \pmod{p^{\delta_1 - \delta_2}}$

Cor (2.1)

$\exists x_0 \in \mathbb{Z}$, $f(x_0) \equiv 0 \pmod{p}$, $f'(x_0) \not\equiv 0 \pmod{p}$

$\Rightarrow \exists x \in \mathbb{Z}_p$, $f(x) = 0$

$a \in \mathbb{Q}_p$, $a = \sum_{n=-m}^{\infty} a_n p^n$ の形, $a = [\dots$

$a_{m-1} a_m]_p$

例]

$\forall m \in \mathbb{N}$, $x^2 + 1 \equiv 0 \pmod{5^m}$ は解を持つか?

\mathbb{Z}_5 で $x^2 + 1 = 0$ の解があるから、はい。

$x = [\dots a_2 a_1 a_0]_{(5)}$ とおくと

$$[\dots a_2 a_1 a_0]_{(5)}^2 = -1$$

$$a_0^2 \equiv 4 \pmod{5}$$

$$(5a_1 + a_0)^2 \equiv 4 \pmod{5^2}$$

⋮

2, 8, 7. \nexists 7, 7.

$$x_0 = 2 \text{ or } 272, \quad f(x) = x^2 + 1 \quad (f'(x) = 2x)$$

$$f(2) = 5 \equiv 0 \pmod{5}, \quad f'(2) = 4 \not\equiv 0 \pmod{5}$$

\rightarrow Hensel $\exists x^2 + 1 = 0$ in \mathbb{Z}_5 or $\overline{\mathbb{F}}_5$.

$$\begin{array}{c} \text{so } \textcircled{1} \quad \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H} \\ \quad \quad \quad \cap \quad \quad \cap \\ \quad \quad \quad \mathbb{Z}_p \subset \mathbb{Q}_p \\ \quad \quad \quad \text{完備化} \end{array}$$

proof.

$$x_i \in \mathbb{Z}_p \quad (i=1, 2, \dots, n) \quad \text{is } \frac{1}{p} \text{ (.)}$$

$$(i) \quad \text{ord}_p(f'(x_i)) = \delta_i, \quad (ii) \quad f(x_i) \equiv 0 \pmod{p^{\delta_i + i - 1}}$$

$$(iii) \quad x_i \equiv x_{i-1} \pmod{p^{\delta_i - \delta_{i-1} + i - 1}}$$

と \exists するから. 構式で書いたら

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)} \quad (\text{Newton 法}) \text{ とおくと}$$

$$f(x_{n+1}) = f\left(x_n - \frac{f(x_n)}{f'(x_n)}\right)$$

→ (1) 展開 →

$$= f(x_n) - f'(x_n) \cdot \frac{f(x_n)}{f'(x_n)} + G_n(x) \left(\frac{f(x_n)}{f'(x_n)} \right)^2$$

より, $G_n(x) = \mathbb{Z}_p$ 上の多項式で表わす。

$$= G_n(x) \left(\frac{f(x_n)}{f'(x_n)} \right)^2$$

(ii) により

$$\text{ord}_p f(x_{n+1}) \geq 2(d_1 + m - d_2) \geq d_1 + m \quad \text{f}$$

(iv) は, $i = m+1$ で成り立つ。

(i) (iv) → 証明

今, $\{x_n\}$ は, \mathbb{Z}_p -列であり (証明)。

\mathbb{Z}_p : 完備より, 収束点 $x \in \mathbb{Z}_p$ がある。

$$\lim_{m \rightarrow \infty} f(x_m) = f\left(\lim_{m \rightarrow \infty} x_m\right) = f(x)$$

2. Hasse-Minkowski の定理 (局所・大域原理) — 2次方程式

(2.1) $\in \mathbb{N}$ かつ $2 \nmid n$ (n が奇数かつ 0)

$K = \text{field}$, $\text{char } K = 0$, $a, b \in K^\times$

$$(a, b)_K = 1 \Leftrightarrow \sqrt{a} \in K \text{ かつ } \sqrt{b} \notin K$$

$$\left\{ \begin{array}{l} b \in \mathbb{N}_{K(\sqrt{a})} \setminus K \quad (1, 1(\sqrt{a})^\times) \end{array} \right.$$

$$(a, b)_K = -1 \Leftrightarrow \sqrt{a} \notin K \text{ or } b \notin N_{K(\sqrt{a})/K} (K(\sqrt{a})^\times)$$

Prop

$$\begin{cases} (a, b)_K = 1 \Leftrightarrow K \perp, ax^2 + by^2 = 1 \text{ has no sol} \\ (a, b)_K = -1 \Leftrightarrow K \perp, ax^2 - by^2 = 1 \text{ has no sol} \end{cases}$$

Rem

$K/\mathbb{Q} =$ finite extension

$$d \in K, N_{K/\mathbb{Q}}(d) = \prod_{\sigma \in \text{Aut } K/\mathbb{Q}} \sigma(d)$$

$$N_{K/\mathbb{Q}}(K^\times) = \{N_{K/\mathbb{Q}}(d) \mid d \in K^\times\}$$

Rem

$$K = \mathbb{Q}_p, (a, b)_{\mathbb{Q}_p} = (a, b)_p \text{ etc}$$

$$\text{lem } a, b \in K^\times$$

$$(1) (a, bc)_K = (a, b)_K (a, c)_K \quad (\text{multiplicativity})$$

$$(2) (a, b)_K = (a, bc^2)_K$$

$$(3) (a, b)_K = (a, b(a-c^2))_K$$

$$(4) a, b \in \mathbb{Z}_p^\times \rightarrow (a, b)_p = 1$$

$$(5) p \mid a, b \in \mathbb{Z}_p^\times \rightarrow (a, b)_p = \left(\frac{a}{p}\right)$$

$$\mathbb{Z}_p^\times = \left\{ \sum_{i=0}^{\infty} a_i p^i \mid \begin{array}{l} 0 \leq a_i < p \\ a_0 \neq 0 \end{array} \right\}$$

11.2.14.25

p : 奇素数

$$\exists x, y \in \mathbb{Z}. p = x^2 + y^2$$

(4) の proof

$$\text{fact } \exists x_0, y_0 \in \mathbb{Z}. ax_0^2 + by_0^2 \equiv 1 \pmod{p} \Leftrightarrow p \equiv 1 \pmod{4}$$

$$f(x, y) = ax^2 + by^2 - 1$$

$$y = y_0 \in \mathbb{Z} \text{ を固定}$$

$$f(x) = ax^2 + by_0^2 - 1$$

$$f(x_0) \equiv 0 \pmod{p}$$

$$f'(x_0) = 2ax_0 \not\equiv 0 \pmod{p}$$

$$\rightarrow \exists x \in \mathbb{Z}_p, f(x) = 0$$

Hensel's lemma

§8.2

$$a \in \mathbb{Z}_p^\times$$

$$(-1)(-1)$$

$$(p, pa)_p = (p, p)_p (p, a)_p$$

$$= (-1, p)_p (-p, p)_p (p, a)_p$$

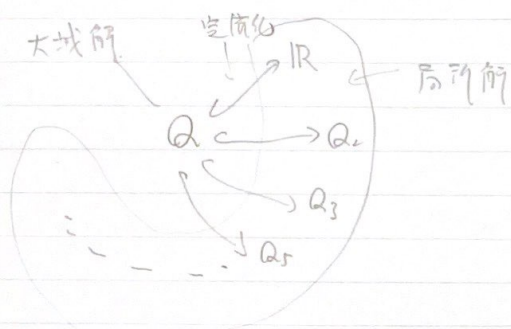
$$= \left(\frac{-1}{p}\right) \left(\frac{a}{p}\right)$$

$$= \begin{cases} \left(\frac{a}{p}\right) & p \equiv 1 \pmod{4} \\ -\left(\frac{a}{p}\right) & p \equiv 3 \pmod{4} \end{cases}$$

2. 局所大域原理

Th.

$$(a, b)_K = 1 \Leftrightarrow (a, b)_{\mathbb{R}} = 1, (a, b)_p = 1$$

 p : 任意の素数

例.

$$\exists x, y \in \mathbb{Q}, p = x^2 + y^2$$

$$x^2 + y^2 = p \Leftrightarrow \frac{1}{p}x^2 + \frac{1}{p}y^2 = 1$$

$$\left(\frac{1}{p}, \frac{1}{p}\right)_\mathbb{Q} = \underbrace{\left(\frac{1}{p}, \frac{1}{p}\right)_\mathbb{Q}}_{\text{大域}}$$

$$\underbrace{\left(\frac{1}{p}, \frac{1}{p}\right)_\mathbb{R}}_1, \underbrace{\left(\frac{1}{p}, \frac{1}{p}\right)_2}_1, \underbrace{\left(\frac{1}{p}, \frac{1}{p}\right)_p}_1, \underbrace{\left(\frac{1}{p}, \frac{1}{p}\right)_q}_1$$

 p : 任意の素数

$$\left(\frac{1}{p}, \frac{1}{p}\right)_p \text{ は 一致しない。}$$

Proof

例

§4. p 進解析の概り.

\mathbb{R} 上では, e^x , $\log x$ があり, $\mathbb{R}(\text{加法群})$, e .

$\mathbb{R}_{>0}(\text{乗法群})$ の間に, $\mathbb{R} \xrightarrow{\log} \mathbb{R}_{>0}$ があった
 $\downarrow \quad \downarrow$
 $x \mapsto e^x$
 $\log x \longleftarrow x+1$

\mathbb{Q}_p 上では, 同じおき \mathbb{Q}_p 型がある

- Def.

$$x \in \mathbb{Q}_p$$

$$\exp_p(x) = \sum_{n=1}^{\infty} \frac{x^n}{n!}$$

$$\log_p(x) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} (x-1)^n$$

- Prop.

$$\exp_p(x) \text{ が収束} \Leftrightarrow x \in p\mathbb{Z}_p$$

$$\log_p(x) \quad " \quad \Leftrightarrow x \in 1+p\mathbb{Z}_p$$

p -adic

$$p^n \mathbb{Z}_p(\text{加法群}) \simeq 1+p^n \mathbb{Z}_p(\text{乗法群})$$

$$\downarrow \quad \downarrow$$

$$x \quad \mapsto \quad \exp_p(x)$$

$$\log x \longleftarrow x+1$$

17)

$$10 \in 1 + 9\mathbb{Z}_3, \quad 10 \notin 1 + 27\mathbb{Z}_3$$

$$\therefore \log_3(10) \in 9\mathbb{Z}_3, \quad \log_3(10) \notin 27\mathbb{Z}_3$$

$$\therefore n \log_3(10) \in 3^{2+nd, n} \mathbb{Z}_3, \quad n \log_3(10) \notin 3^{3+nd, n} \mathbb{Z}_3$$

$$\therefore \log_3(10^n) \in 3^{2+nd, n} \mathbb{Z}_3, \quad \log_3(10^n) \notin 3^{3+nd, n} \mathbb{Z}_3$$

$$\therefore 10^n - 1 \in 3^{2+nd, n} \mathbb{Z}_3, \quad 10^n - 1 \notin 3^{3+nd, n} \mathbb{Z}_3$$

$$\therefore \text{ord}_3(10^n - 1) = 2 + nd, n$$

$$\therefore \text{ord}_3\left(\frac{10^n - 1}{9}\right) = nd, n$$